3GPP TSG SA WG3 Security — S3#21 **S3-010701**

27 - 30 November, 2001

Sophia Antipolis, France

Source:	**AT&T Wireless/Alcatel**
Title:	**CR to 33.203: Network Hiding Mechanism**
Agenda item:	Hiding
Document for:	APPROVAL

Following discussions on contributions S3-010586 (AT&T Wireless) and S3-010653(Alcatel), it is proposed that the following modifications to be made in section 6.4 of 33.203.

6.4 Hiding mechanisms

The Hiding Mechanism is optional for implementation. All I-CSCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF shall encrypt the ~~address of the S-CSCF~~hiding information elements when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF shall decrypt those information elements that were encrypted by I-CSCF in this hiding network domain. ~~An IV of 128-bit is needed at the encryption and decryption phase and it shall be appended to the encrypted information. The information shall also be MAC protected with a block cipher in CBC-MAC mode.~~

~~When the I-CSCF decrypts the information it shall verify the integrity.~~

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode shall be used. The network hiding mechanism will not address the issues of authentication and integrity protection of SIP headers. The AES in CBC mode with 128-bit block and 128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. Therefore, random IV shall be used for each encryption. The same IV is required to decrypt the information. The IV shall be included in the same SIP header that includes the encrypted information.

Editor's note: the following open issues are still to be resolved: user of a key identifier for the support of multiple encryption secret keys; possible use of a MAC to protect integrity of the resulting cipher text; impact of IV field value on compressibility of incoming SIP messages; key management and distribution amongst I-CSCFs; implications onto development of SIP are to be considered.